L Number	Hits	Search Text	DB	Time stamp
1	1184	(382/100).CCLS.	USPAT; US-PGPUB; IBM_TDB	2004/05/04 09:54
2	138	((382/100).CCLS.) and tamp$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 09:55
3	61	(((382/100).CCLS.) and tamp$4) and hash	USPAT; US-PGPUB; IBM_TDB	2004/05/04 09:55
4	50	((((382/100).CCLS.) and tamp$4) and hash) and display$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:22
5	79	combine$4 near5 imag$4 near4 mark	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:18
6	3	(combine$4 near5 imag$4 near4 mark) same cod$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:19
7	12074	cod$4 same encrypt$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:23
8	1015	(cod$4 same encrypt$4) same imag$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:23
9	31	((cod$4 same encrypt$4) same imag$4) same multiplex$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:33
10	932	mark with image with input	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:34
11	1	(mark with image with input) same hash	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:34
13	0	((mark with image with input) same cod$4) same encrypt$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:34
12	73	(mark with image with input) same cod$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 10:35

L Number	Hits	Search Text	DB	Time stamp
1	297	image near5 tamper$3	USPAT; US-PGPUB; IBM_TDB	2004/05/04 13:56
2	19	(image near5 tamper$3) same hash	USPAT; US-PGPUB; IBM_TDB	2004/05/04 13:55
3	73	(image near5 tamper$3) same (stamp$3 sign$3 mark$3)	USPAT; US-PGPUB; IBM_TDB	2004/05/04 14:45
5	4	(imag$4 same cod$4 same hash same (mark sign$4 stamp$3) same encrypt$4) same multip$5	USPAT; US-PGPUB; IBM_TDB	2004/05/04 14:46
4	50	imag$4 same cod$4 same hash same (mark sign$4 stamp$3) same encrypt$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 14:52
6	4	dispaly$4 same cod$4 same imag$3	USPAT; US-PGPUB; IBM_TDB	2004/05/04 14:53
7	16286	display$4 same cod$4 same imag$3	USPAT; US-PGPUB; IBM_TDB	2004/05/04 14:53
8	15	(display$4 same cod$4 same imag$3) same hash	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:09
9	35	imag$4 near5 tamper$3 near4 (stamp sign$5 mark$4)	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:23
10	59938	imag$4 same cod$4 hash same encrypt$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:24
11	15399	(imag$4 same cod$4 hash same encrypt$4) same transm$7	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:25
12	85	((imag$4 same cod$4 hash same encrypt$4) same transm$7) same tamper$3	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:48
13	0	coded near5 imag$4 near7 dispaly$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:55
14	801	coded near5 imag$4 near7 display$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:56
15	517	coded near2 imag$4 near7 display$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:56
16	1	(coded near2 imag$4 near7 display$4) same tamper$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:58
17	2	(coded near2 imag$4 near7 display$4) same (watermark$$ steganograph$4 tamper$4)	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:57
19	1	((coded near2 imag$4 near7 display$4) same transmi$7) same hash	USPAT; US-PGPUB; IBM_TDB	2004/05/04 15:58
18	132	(coded near2 imag$4 near7 display$4) same transmi$7	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:14
21	3	(hash same imag$4 same cod$4 same encryp$4) same tamper$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:19
20	76	hash same imag$4 same cod$4 same encryp$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:16
22	54	(hash same imag$4 same cod$4 same encryp$4) and tamper$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:25
23	5	imag$4 near5 tamper$4 near4 display$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:26

24	311	imag$4 near5 tamper$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:26
25	14	(imag$4 near5 tamper$4) near5 cod$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:33
26	0	"10482074"	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:35
27	1651	hash adj3 key	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:35
28	1849984	sign$3 mark$3 stamp$3	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:43
29	3	multiplex$3 same hash same cod$4 same encrypt$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:38
30	125894	(sign$3 mark$3 stamp$3) near5 cod$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:43
31	937	((sign$3 mark$3 stamp$3) near5 cod$4) with encrypt$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:44
33	2	((((sign$3 mark$3 stamp$3) near5 cod$4) with encrypt$4) with imag$4) same hash	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:44
32	130	(((sign$3 mark$3 stamp$3) near5 cod$4) with encrypt$4) with imag$4	USPAT; US-PGPUB; IBM_TDB	2004/05/04 16:45

US 20020012445 A1

TITLE: Authentication watermarks for printed objects and related applications

---------- KWIC ---------

Detail Description Paragraph - DETX (52):

[0063] Similar techniques may be used to create a fragile watermark that evidences copying due to changes in the fragile watermark's strength relative to its original strength in the un-manipulated original printed object. Also, the fragile watermarks may be adapted to carry a message payload. Finally, the fragile watermarks may be spatially replicated in contiguous blocks of the image. The detector can then isolate the spatial location of blocks of the **image where the fragile watermark or watermarks evidence tampering**

RE38236

DOCUMENT-IDENTIFIER: US RE38236 E

TITLE: Digital signal transmitting method, digital signal receiving apparatus, and recording medium and method

---------- KWIC ---------

Claims Text - CLTX (1):

1. A method for transmitting a digital signal, comprising the steps of:

band-compression **coding** a first digital signal and a second digital signal, each respective digital signal defining an **image**; **encrypting** the band-compression **coded** first digital signal; **multiplexing the encrypted** first digital signal and the band-compression **coded** second digital signal; and **encrypting the multiplexed** first and second digital signals to form said digital signal for transmission.

Claims Text - CLTX

US-PAT-NO: 6532541

DOCUMENT-IDENTIFIER: US 6532541 B1
See image for Certificate of Correction

TITLE: Method and apparatus for image authentication

---------- KWIC ---------

Brief Summary Text - BSTX (7):

The first method employs an **encrypted** digital signature which is generated by the **image** capturing device. Generally, the digital signature is based on a public key **encryption** method. In this type of method, a private key, known only to the capturing device, is used to **encrypt** a hashed version of an **image** to form the "signature" of the **image** which travels with the **image**. A public key is used to decrypt the signature. The public key is also used to **hash the image** and compare the **codes** of the current **image** to the original signature. If the **codes** match, the present **image** is considered authentic

A

TITLE: Electronic signature method and apparatus

---------- KWIC ---------

Detailed Description Text - DETX (6):
Thereafter, a signature **image** G is **encrypted with a key of the hash value H corresponding to a secret-key** cryptosystem. Then an **encryption** function A is transformed with the hash value H.

Detailed Description Text - DETX (21):
The signature **image** transforming means 15 **encrypts** the signature **image** G received from the signature **image** input means 11 with a **key of the hash value H received from the hashing means 14 corresponding to a method of a secret-key** cryptosystem and sends the **encrypted** result to signature document generating means 16. Accordingly, at step S13 of FIG. 1a, a transform value is generated from the signature **image** G to a **encryption** function A with the hash value H according to the **encrypted** function A=f1(G, H).

Claims Text - CLTX (11):

US-PAT-NO: 6005936

DOCUMENT-IDENTIFIER: US 6005936 A
See image for Certificate of Correction

TITLE: System for embedding authentication information into an image and an image alteration detecting system

---------- KWIC ---------

Brief Summary Text - BSTX (7):

FIG. 1 is a block diagram of the **image** processing system of the conventional digital camera. A photographed object is converted to an electric analog signal by a CCD 12 through an optical system 11. This signal is processed by a signal processing unit 13, and outputted as **image** data D which is a digital signal. The generated **image** data D is inputted to a digest calculating unit 14. The digest calculating unit 14 calculates a hash value H of the data of the whole **image**. The hash value is a value (digest) uniquely determined by a calculation based on the **image** data and showing the characteristics of the **image**. The hash value H as a digest depends on the **image** contents. An **encrypting** unit 15 **encrypts the hash value H**

6425081

DOCUMENT-IDENTIFIER: US 6425081 B1
See image for Certificate of Correction

TITLE: Electronic watermark system electronic information distribution system and image filing apparatus

---------- KWIC ---------

Detailed Description Text - DETX (52):
Various data, to include **image** data in the first and the second embodiment and a hash value obtained during the embedding process for an electronic watermark, can be stored in the following **image** format. According to the following general **image** format, for example, **image** data that are transmitted at individual steps can be stored in an **image** data portion, and a corresponding hash value and its signature can be stored in an **image** header portion. Furthermore, a **hash value and its signature, which the user must retain, and the secondary encryption key** can be stored in the **image** header portion, while **image** data having an electronic watermark can be stored in the **image** data portion.

US-PAT-NO: 6278791

DOCUMENT-IDENTIFIER: US 6278791 B1

TITLE: Lossless recovery of an original image containing embedded data

---------- KWIC ---------

Detailed Description Text - DETX (31):

The **hash** value h is then directed to an **encryption** circuit 44. A string of values called an **encryption** key is also directed to the **encryption** circuit 44. The **encrypted** signal produced by circuit 44 resembles a random bit stream and is called the digital signature s of the original **image** I(x, y). In a cryptographically strong system, it is computationally infeasible to generate the correct signature without knowledge of the key. By making the **encryption** key available only to the authorized users (i.e., a private key), it can be assured that the signature cannot be duplicated by any unauthorized user. A variety of **encryption** methods are possible, including, a commercially available product from RSA Data Security Inc. called RC-4.TM.. Further examples of

US-PAT-NO: 6620047

DOCUMENT-IDENTIFIER: US 6620047 B1

TITLE: Electronic gaming apparatus having authentication data sets

---------- KWIC ---------

Detailed Description Text - DETX (19):

When a software release is ready for shipment, a **HASH** function designed for cryptographic use generates a unique fixed-length string of 128 bits for the loadable **code image**. This string, called a message digest, is then **encrypted** using RSA software and the proprietor's private key to produce a digital signature for the **image**. The signature is then written to disk with the loadable **code image**. When the **code image** is loaded from the disk and is ready to be executed during the system boot sequence, the secure loader decrypts the digital signature using the public key stored in ROM. The secure loader verifies that the **image** is authentic by comparing the message digest computed for the loadable **code image** with the message digest decrypted from disk. The

PGPUB-DOCUMENT-NUMBER: 20020007456

PGPUB-FILING-TYPE: new

DOCUMENT-IDENTIFIER: US 20020007456 A1

TITLE: Secure processor architecture for use with a digital rights management (DRM) system on a computing device

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	STATE	COUNTRY	CITY RULE-47
Peinado, Marcus	WA	US	Bellevue
England, Paul	WA	US	Bellevue

US-CL-CURRENT: 713/164

ABSTRACT:

A secure processor is operable in normal and preferred modes, and includes a security kernel instantiated when the processor enters into preferred mode and a security key accessible by the security kernel during preferred mode. The security kernel employs the accessed security key to authenticate a secure application, and allows the processor to be

US-PAT-NO: 6357004

DOCUMENT-IDENTIFIER: US 6357004 B1

TITLE: System and method for ensuring integrity throughout post-processing

---------- KWIC ---------

Detailed Description Text - DETX (30):
MOS value(s) 750.sub.4 specifies what operation(s) was (were) performed on the data. For example, one MOS value might indicate "background color changed to blue", while another might indicate "font style changed to 8-point Times", while yet another might indicate "**image** scaled by 132%". The outgoing hash value 750.sub.5 provides sufficient information for verification of the post-processed data produced by the manipulation agent by performing a hash operation of the data. The extended digital signature 750.sub.6 is produced by hashing the data after post-processing operations were completed, referred to as an "outgoing **hash value", and encrypting the outgoing hash value under the private key** of the manipulation agent. The outgoing hash value may be used to provide sufficient information for

US-PAT-NO: 4261018

DOCUMENT-IDENTIFIER: US 4261018 A

TITLE: Progressive image transmission

---------- KWIC ---------

Brief Summary Text - BSTX (6):

What is desired is a progressive picture display which at the same time achieves a significant compression. The basic advantage of progressive **display of binary pictures over line-by-line display** is that in early stages of reconstruction one sees the entire image in crude form, instead of seeing only the top part in final form.

Claims Text - CLTX (18):

9. In an image transmission system (FIG. 1) including at a transmitting terminal a scanning device (10), an addressable memory (11) for storing black and white binary values corresponding to each picture element of an **image to be transmitted, a transmission channel (15) for such image at a receiving terminal, an image display device (20), and**